SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

CASUAL ACCESS APPLICATION WITH CONTEXT SENSITIVE PIN AUTHENTICATION

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention is directed to user authentication in an exchange environment. Specifically the invention is directed to a method and system for allowing access to an exchange by a casual user without compromising exchange security.

DESCRIPTION OF THE RELATED ART

[0002] It is known to have an electronic exchange configured such that various buyers and sellers of goods and/or services can come together and conduct business. In such an exchange, several applications may be running in a protected environment. To participate in the exchange and to have full access to the exchange applications one must be a registered member. Registration requires completion of a complex procedure in which a prospective member must submit a large quantity of information which then must be validated before membership is authorized. This complex procedure deters casual users from participating in the exchange and thus prevents the exchange from obtaining necessary information from such casual users. A casual user is defined as one who may not need full access to the exchange and its applications, but may only need to complete simple business transactions. For example, an organization may be a member of the exchange via the membership of its procurement employee. Under that organization's policies, the procurement employee is authorized to make purchases on behalf of the organization for under a

certain amount. If the cost of a purchase is over that certain amount, it is necessary for that procurement employee to get additional authorization from his or her manager. This manager, however, may not be registered to participate in the electronic exchange or to use its applications. In order to complete the transaction, that manager's authorization is necessary. Thus, it is desirable to allow the manager to have access as a casual user for the limited purpose of providing the necessary authorization.

[0003] In addition to reducing the complexity of authorization when allowing access to casual users, it is also important to maintain the exchange's security and to avoid possible breaches. Therefore, the inventors have determined that there is a need for a simple yet secure way to provide access to casual users on an electronic exchange.

SUMMARY OF THE INVENTION

[0004] The present application describes a method of providing a casual user access to an electronic exchange via interaction with a casual access application. The method comprises: receiving a request from an external application; generating and transmitting an external message to the casual user containing information on accessing the casual access application; generating a context sensitive personal identification number (CS-PIN) upon access of the casual access application by the casual user using the information contained in the external message; storing the CS-PIN in a CS-PIN holder accessible to the casual user; and completing the request upon access by the casual user using the CS-PIN.

[0005] In addition, the present application describes a system for providing a casual user access to an electronic exchange. The system comprises: an exchange application server for running exchange applications, at least one of the applications requiring interaction with the casual user; a casual access application server connected to the exchange application server for receiving a request from and for transmitting a response to the exchange application server, for generating an external message for the casual user containing information on accessing the casual access application server, for generating a context sensitive personal identification number (CS-PIN) for the casual user and for completing the request through interaction with and upon access by the casual user; and a CS-PIN holder accessible by the casual user and

connected to the casual access application server for receiving a CS-PIN from the casual access application server and providing it to the casual user.

[0006] Other features and advantages of the present invention will become apparent to those skilled in the art from the following detailed description. It should be understood, however, that the detailed description and specific examples, while indicating preferred embodiments of the present invention, are given by way of illustration and not limitation. Many changes and modifications within the scope of the present invention may be made without departing from the spirit thereof, and the invention includes all such modifications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The foregoing advantages and features of the invention will become apparent upon reference to the following detailed description and the accompanying drawings, of which:

[0008] Figure 1 is a case diagram illustrating the use of the casual access application with context sensitive PIN authentication; and

[0009] Figure 2 illustrates a typical configuration for a casual access application in interaction with an exchange application.

DETAILED DESCRIPTION OF THE INVENTION

[0010] The present invention is now described in detail with reference to the above-mentioned figures. The present invention can be summarized as a method and system for allowing access to an exchange by a casual user without compromising exchange security. This allows a casual user to provide required input and complete simple business transactions without becoming a registered member of the exchange. The system knows what information to provide to or to collect from the casual user and provides him with a context sensitive personal identification number (CS-PIN) to allow access for that purpose and to restrict access for other purposes. The benefits derived from this invention include one or more of maintaining a secure exchange application, reducing the exchange maintenance costs, for example, in help desk employees, reducing user error by limiting the casual user's exposure to the applications, lowering operational costs, reducing the cycle times of business processes and

reducing human resources costs.

[0011] Figure 1 is a case diagram illustrating the use of the casual access application with context sensitive PIN authentication. This figure shows the method of the present invention and the interaction between the various applications and participants. In this figure the exchange application (EA) represents any application that is protected by the exchange security mechanisms and requires an external participant (EP) to access all or a subset of its features. The external participant (EP), also called a "casual user," represents any individual who is required to interact with an exchange application but is not registered with the exchange security mechanisms. Typically, the external participant would be represented by a PC, a PDA or other network or Internet device.

[0012] Starting with the upper left corner of Figure 1, some event takes place within the exchange application wherein the application determines that some interaction with an external participant is necessary. For example, the application may need some input from the external participant, or the external participant may need to access some information from the application. Once this determination is made, a new external request is created, as shown as box 10 in Figure 1. In this step certain information is transferred from the exchange application to a casual access application (CAA) (shown in Figure 2 as block 250). This may be a form that is passed from the exchange application to the CAA or it may just be a request from the exchange application to the CAA to use an existing template along with information to fill out different variables within the template.

[0013] The CAA 250 receives this request and will do three things. The first, shown in box 20, is to generate a reference such as a unique URL. This reference is going to be the address that the external participant will use in order to access the CAA 250. At the same time the CAA, as shown in box 30, stores the data received from the exchange application for later reference. Once the reference is generated the external participant is notified, as shown in box 40. This notification includes the reference that was generated plus any other message that the external participant will need in order to access the CAA.

[0014] This notification is then given to a messaging application (MA) which is a mechanism for sending messages to individuals that may or may not be registered

with the exchange security mechanisms. The notification is communicated as shown in box 50 by the messaging application to the external participant. In the preferred embodiment this is done via e-mail, but in the present invention can include any other form of communication. More important than the form of communication used is the fact that the notification includes the information needed for the external participant to access the CAA system, including the reference.

[0015] As shown in the figure the external participant is able to login to the CAA 250 using the reference it has received, as shown in box 60. Once he has logged in, the CAA will acknowledge his entrance into the system and inform him that a context sensitive PIN will be generated. Box 70 shows the actual generation of the CS-PIN by the CAA. Note that the actual CS-PIN is not communicated to the external participant, but rather only a notification that a CS-PIN has been generated is communicated. Also, in the preferred embodiment of the invention, the CS-PIN itself is time sensitive in that it will expire within a certain amount of time if not used or retrieved.

[0016] The CS-PIN, as shown in box 80, is sent by the CAA and is stored with a CS-PIN holder (PH). This CS-PIN holder represents a location that is well known to both the exchange and the external participant. This location is where the CS-PIN is deposited by the system in order to provide it to the external participant when requested. There are several possible implementations of the CS-PIN holder. For example, it could be an e-mail address wherein the CS-PIN itself is e-mailed to that address. It could also be a globally accessible web page wherein the CS-PIN is published. It could also be a globally accessible FTP server wherein the CS-PIN is uploaded to that server. Essentially the CS-PIN holder could be any system to which the CAA services are allowed to write data and the external participant has read permission. The CS-PIN holder could remain the same for future accesses by the external participant and could even be located with the external participant. Alternatively, the CS-PIN holder could change from access to access, thus being valid for only one transaction, thereby making the system more secure.

[0017]

The external participant, once notified that a CS-PIN has been generated, can retrieve this CS-PIN, as shown in box 90, from the CS-PIN holder. As mentioned above, the CAA application does not inform the external participant of the location of

the CS-PIN holder or how to access it. This information must be obtained by the external participant from the registered user or another credentialed source. Thus, the registered user is responsible for contacting the external participant to establish the location and possibly the type of the CS-PIN holder to be used. In this way no message transmitted to the external participant from the CAA system contains sufficient information to allow an unauthorized interceptor of a message to access the system. For instance, while an intercepted message may contain the generated URL or other reference to access the CAA system, such message would not contain the CS-PIN or the location of the CS-PIN holder.

[0018] Referring again to Figure 1, once the external participant has, in box 90, retrieved the CS-PIN from the CS-PIN holder, he can then access the forms that he needs to access in order to provide the information needed by the application or to see the information he needs to see. This is shown in box 100. The CAA, in box 110, validates the CS-PIN to positively identify the external participant. The request data previously stored, is shown in box 120 as being retrieved in order to provide the external participant with the requisite information or requisite questions to answer.

[0019] After the external participant has completed what is necessary from him, he submits the form, as shown in box 130, and the CAA will log him out of the system. The request data will be removed by the CAA from the active database, as shown in box 140. The CAA will then notify the exchange application appropriately, as shown in box 150. That is, the exchange application will be provided with the necessary information obtained from the external participant or derived from that information. This may include information provided by the external participant or simply an indication that the external participant has viewed certain information or has provided authorization by electronic signature, etc.

[0020] Figure 2 shows a typical configuration for a CAA server in interaction with an exchange application server. The exchange application server, shown as element 210, submits a business form via a secured tunnel, shown as 220. This form, as discussed above, could be a template, but more generally is the request for information needed from the external participant. The secured tunnel used to communicate this request to the CAA server traverses the exchange security, shown as element 240. The

connection between the exchange application server 210 and the CAA server 250 could be any number of secure communication links and is preferably a direct connection. Similarly, the response ultimately provided by the CAA server 250 to the exchange application 210 is made via a secured tunnel 230, which also traverses the exchange security 240.

[0021] The CAA server 250 performs all of the functions attributed to the CAA as described above with reference to Figure 1. The functionality of the system could be implemented in a CAA server using a single processor, multiple processors or using several processor systems that are connected over a network. It is also possible to distribute the functionality of the system over a multitude of sites which are suitably connected together using conventional networking or inter-networking techniques.

[0022] As discussed above, the CAA server interacts with the casual user or external participant shown as element 270 using one or more appropriate protocols, as well as with the CS-PIN holder shown as well known location 275. The casual user 270 is represented as a computer, but could also be interacting with the system by hand held devices or other convenient devices. The CS-PIN generated by the CAA server 250 is deposited with the well known location 275 over a link 260. The characteristics of link 260 depend upon the implementation of the CS-PIN holder or well known location 275.

[0023] In addition, the casual user 270 must interact with well known location 275. This interaction is made over link 285, the characteristics of which also depend upon the implementation of well known location 275. Having obtained the CS-PIN from the well known location 275, the casual user 270 can access the requisite forms from CAA server 250. This access is made via link 280, which in the preferred embodiment is Internet based. In fact, links 260, 280 and 285 may all be Internet based, the Internet being shown in Figure 2 as element 290.

[0024] In the preferred embodiment, the element 290 is the Internet. However, element 290 can also include a wide area network (WAN), an internet network, a public tariff telephone network or a private value added network (VAN). Alternatively, element 290 can be implemented using any combination of these different kinds of communication networks. It will be appreciated that many other similar configurations are within the

abilities of one skilled in the art and all of these configurations could be used with the method of the present invention. Furthermore, it should be recognized that the computer system and network disclosed herein can be programmed and configured in a variety of different manners by one skilled in the art, to implement the method steps discussed further herein.

[0025] Thus, a method and system for allowing access to an exchange by a casual user without compromising exchange security have been described according to the present invention. Many modifications and variations may be made to the techniques and structures described and illustrated herein without departing from the spirit and scope of the invention. Accordingly, it should be understood that the methods and interfaces described herein are illustrative only and are not limiting upon the scope of the invention.

[0026] It should be noted that although the flow chart provided herein shows a specific order of method steps, it is understood that the order of these steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen in generally on designer choice. It is understood that all such variations are within the scope of the invention. Likewise, software and web implementation of the present invention could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various database searching steps, correlation steps, comparison steps and decision steps.